Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Cyberbeveiligingswet

Zorgplicht

In Nederland wordt de Europese NIS2-richtlijn geïmplementeerd in de vorm van de Cyberbeveiligingswet (Cbw). Deze wet is gericht op de verbetering van de digitale weerbaarheid van belangrijke en essentiële diensten en organisaties. De Cbw schrijft drie verplichtingen voor: de zorgplicht, registratieplicht en meldplicht.

Deze infosheet gaat in op de zorgplicht.

Wat is de zorgplicht?

Essentiële en belangrijke entiteiten moeten maatregelen nemen om hun netwerk- en informatiesystemen tegen incidenten te beschermen. Hetzelfde geldt voor de fysieke omgeving waarin de systemen zich bevinden.

Moet mijn organisatie voldoen aan de zorgplicht?

Onder de Cbw vallen entiteiten die bij uitval van diensten zorgen voor een ontwrichtende impact op de economie en de samenleving. Hierbij wordt onderscheid gemaakt tussen ‘essentiële’ en ‘belangrijke’ entiteiten. De zorgplicht geldt voor alle organisatie die volgens de Cbw essentieel of belangrijk zijn.

Via www.ncsc.nl/NIS2 kom je er snel achter of jouw organisatie hieronder valt.

Zijn alle maatregelen van toepassing op mijn organisatie?

De Cbw schrijft voor dat de maatregelen passend en evenredig moeten zijn. Bij de beoordeling van de evenredigheid kun je kijken naar de mate waarin jouw organisatie is blootgesteld aan risico’s, de omvang van de organisatie, de kans dat zich incidenten voordoen en de mogelijke impact op de maatschappij en economie.

Wie is verantwoordelijk voor het naleven van de zorgplicht?

Het bestuur van de organisatie is eindverantwoordelijk voor het naleven van de zorgplicht. Zij kunnen voor het niet naleven aansprakelijk worden gesteld. Er ligt een actieve rol voor hen weggelegd in het goedkeuren van de voorgenomen maatregelen, het houden van toezicht op de implementatie, het volgen van training om kennis te vergroten en het aanbieden van trainingen aan medewerkers.

Kijk voor meer informatie op www.ncsc.nl.

Versie: september 2025

Aan de slag

Het is primair van belang dat een organisatie kan aantonen op passende wijze in control te zijn over haar (digitale) weerbaarheid. De Cbw kent 10 zorgplichtmaatregelen.

1. Maak een risicoanalyse

De eerste essentiële stap voor het verkrijgen van nodige inzichten. Uit een risicoanalyse komt naar voren welke risico's het zwaarst wegen en waar beveiligingsmaatregelen het hardst nodig zijn.

2. Versterk de beveiliging op het gebied van personeel, toegang en assetbeheer

Weet wie toegang heeft tot welke informatie. Door deze 'eerste verdedigingslinie' tegen cyberaanvallen serieus te nemen, verbeter je de cyberbeveiliging van netwerk- en informatiesystemen.

3. Maak een Bedrijfscontinuïteitsplan (BCP)

Voor de meeste bedrijven is (langdurige) uitval van primaire bedrijfsprocessen onacceptabel. Een bedrijfscontinuïteitsplan (BCP) helpt je veerkrachtig te zijn bij onverwachte gebeurtenissen zoals stroomuitval, cyberincidenten en -aanvallen.

4. Richt Incident Response in

De gevolgen van verstoringen, uitval, datalekken of cyberaanvallen kunnen ernstig zijn. Daarom is het cruciaal om bij een incident adequaat te reageren om negatieve gevolgen te beperken. Een Incident Response Plan (IRP) helpt je hierbij.

5. Zorg dat cyberhygiëne op orde is

Met een goede cyberhygiëne hanteert de gehele organisatie de basisprincipes van cyberveiligheid. Het trainen en informeren van werknemers is essentieel voor het naleven van deze basispraktijken.

6. Schrijf beleid op de beveiliging van netwerk- en informatiesystemen

Veel bedrijven en organisaties zijn afhankelijk van netwerk- en informatiesystemen voor hun primaire bedrijfsprocessen. Als je geen toegang hebt tot deze systemen of als informatie openbaar wordt, kan dit grote gevolgen hebben voor de organisatie.

7. Maak je toeleveringsketen veilig

Bedrijven zijn vaak afhankelijk van de producten of diensten van toeleveranciers. Digitale verbindingen tussen bedrijven vergroten deze afhankelijkheid. Daarom is het van belang maatregelen te nemen om de toeleveringsketen te beveiligen.

8. Maak beleid op cryptografie en encryptie

Cryptografie en encryptie vormen de basis voor de vertrouwelijkheid en integriteit van jouw bedrijfsgegevens en assets. In een beleidsdocument beschrijf je de technieken en maatregelen die je neemt om deze vertrouwelijkheid en integriteit te beschermen.

9. Gebruik MFA of andere beveiligde authenticatieoplossingen

Voor veilige bedrijfsprocessen is het essentieel dat gebruikers, apparaten en andere activa worden geauthentiseerd met meerdere authenticatiefactoren (MFA) of continue authenticatiemechanismen om toegang te krijgen tot de netwerken en informatie-systemen van de organisatie.

10. Hanteer processen om de effectiviteit van maatregelen te beoordelen

Het beoordelen van de effectiviteit van cyberveiligheidsmaatregelen is essentieel. Het helpt risico's te beheren, zorgt voor naleving van wetten en identificeert verbeterpunten. Dit proces bouwt vertrouwen bij stakeholders en maakt aanpassing aan nieuwe bedreigingen mogelijk.

Kijk voor meer informatie op www.ncsc.nl.